

AMENDMENT AND PRESENTATION OF CLAIMS

Please replace all prior claims in the present application with the following claims, in which claims 20-37 are currently amended, and claims 38-40 are newly presented.

1.-19. (Cancelled)

20. (Currently Amended) A ~~digital information security system for providing security,~~ the system comprising:

a user application tool configured to be installed in a user terminal, the user application tool being structured further configured to create a unique user key using unique system information of the user terminal, ~~to transmit wherein~~ the unique user key is transmitted to a server system for authentication, ~~via a network for registration and to subsequently transmit the unique user key to the server system via the network for authentication;~~

~~the server system comprising an encryption unit to encrypt digital information, a user information database to store the user information including the unique user key received from the user terminal for registration, a digital information database to store the encrypted digital information, a rule establishing unit to establish a rule corresponding to the user information and the digital information, a coupling unit to encrypt, using the unique user key, rule information corresponding to the rule, to encrypt, using the unique user key, a decryption key for decrypting the digital information, and to combine the encrypted rule information, the encrypted decryption key and the encrypted digital information into combined information, and a digital file database to store the combined information; and~~

~~the server system also comprising a server control unit including a user management tool to perform a user authentication process by comparing the unique user key stored in the user information database with the unique user key subsequently transmitted from the user terminal for authentication,~~

~~wherein the server control unit transmits the combined information from the digital file database to the user application tool after completing the user authentication process, when the user terminal requests a download of the digital information.~~

21. (Currently Amended) The ~~digital information security~~ system as claimed in claim 20 38, wherein when the combined information is downloaded to the user application tool, it is determined whether ~~the a~~ digital file should be decrypted by determining whether ~~the a~~ key used for encrypting the decryption key matches the unique user key created by the user application tool.

22. (Currently Amended) The ~~digital information security~~ system as claimed in according to claim 20 38,

wherein the rule establishing unit establishes a rule for one or more of authority of storage, authority of print, authority of allowable time for use, ~~and or~~ authority of transfer of the digital file.

23. (Currently Amended) The ~~digital information security~~ system as claimed in according to claim 20, wherein the system information includes ~~wherein the unique system information includes~~ at least one of unique CPU (Central Processing Unit) information, RAM

(Random Access Memory) information, unique HDD (Hard Disk Drive) information, and or serial number information of the user terminal.

24. (Currently Amended) A ~~digital information security~~ method for providing security, the method comprising the steps of:

creating a unique user key using ~~unique~~ system information of a user terminal ~~using a user application tool installed in a user terminal; and~~

~~transmitting digital information and user information including the unique user key from the user terminal to a server system via a network, wherein the unique user key is transmitted by a user application tool installed in the user terminal for authentication.~~

~~encrypting the digital information and the user information including the unique user key transmitted from the user terminal;~~

~~storing the encrypted user information and the encrypted digital information in the server system;~~

~~establishing a rule corresponding to the user information and the digital information; encrypting the rule and a decryption key for decrypting the digital information using the unique user key;~~

~~-combining the encrypted digital information, the encrypted rule and the encrypted decryption key into combined information;~~

~~storing the combined information;~~

~~performing a user authentication process by comparing the unique user key stored in the server with the unique user key subsequently transmitted from the user application tool of the user terminal for authentication;~~

~~transmitting the combined information from the server system to the user application tool via the network after completing the user authentication process, when the user terminal requests a download of the digital information; and~~

~~determining, with the user application tool, whether the digital file should be decrypted by determining whether the key used for encrypting the decryption key matches the unique user key created by the user application tool.~~

25. (Currently Amended) The ~~digital information security~~ method as ~~claimed in~~ according to claim 24 39, wherein the rule includes one or more of authority of storage, authority of print, authority of allowable time for use, and or authority of transfer of the data.

26. (Currently Amended) The ~~digital information security~~ method as ~~claimed in~~ according to claim 24, wherein the ~~unique~~ system information includes at least one of unique CPU (Central Processing Unit) information, RAM (Random Access Memory) information, ~~unique~~ HDD (Hard Disk Drive) information, and or serial number information of the user terminal.

27. (Currently Amended) A ~~digital information encryption and upload~~ method comprising the steps of:

A method for uploading data, the method comprising:

creating a unique user key using ~~unique~~ system information of a user terminal using a user application tool installed in a the user terminal;

uploading ~~digital information data, and~~ user information from the user terminal to a server system, the user information including the unique user key ~~from the user terminal to a server system~~ ;

encrypting the ~~digital information data~~ and the user information including the unique user key transmitted from the user terminal;

storing the encrypted user information and the encrypted ~~digital information data~~ in the server system;

establishing a rule corresponding to the user information and the ~~digital information data~~;

encrypting the rule and a decryption key for decrypting the digital information using the unique user key;

combining the encrypted decryption key, the encrypted ~~digital information data~~, and the encrypted rule into a combined file; and

storing the combined file.

28. (Currently Amended) The ~~digital information encryption and upload~~ method as ~~claimed in according to~~ claim 27, wherein the rule includes one or more of authority of storage, authority of print, authority of allowable time for use, ~~and or~~ authority of transfer of the ~~digital information data~~.

29. (Currently Amended) The ~~digital information encryption and upload~~ method as claimed in according to claim 27, wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, RAM (Random Access Memory) information, unique HDD (Hard Disk Drive) information, and or serial number information of the user terminal.

30. (Currently Amended) ~~An encrypted digital information download method comprising the steps of:~~

A method for downloading data, the method comprising:

creating a ~~unique~~ user key using unique system information of a user terminal using a user application tool installed in a the user terminal;

transmitting a request from the user terminal to a server system to download ~~digital information data~~ from the server system; and

transmitting the unique user key from the user terminal to the server system;

~~performing a user authentication process at the server system by comparing a unique user key stored in the server system with the unique user key transmitted from the user terminal;~~

~~transmitting a digital file from the server to the user terminal when the user terminal is authenticated, the digital file including an encrypted version of the digital information and an encrypted decryption key, the decryption key for decrypting the encrypted version of the digital information; and~~

~~decrypting, at the user terminal, the encrypted version of the digital information if the key used for encrypting the decryption key matches with the unique user key created by the user application tool.~~

31. (Currently Amended) The ~~digital information download~~ method as claimed in according to claim 30 40, further comprising:

establishing a rule associated with the ~~digital information~~ data, wherein the rule includes one or more of authority of storage, authority of print, authority of allowable time for use, and or authority of transfer of the digital information;

wherein the ~~digital~~ file includes an encrypted version of the rule.

32. (Currently Amended) The ~~digital information download~~ method as claimed in according to claim 30, wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, RAM (Random Access Memory) information, unique HDD (Hard Disk Drive) information, and or serial number information of the user terminal.

33. (Currently Amended) A ~~digital information security method in a system in which a digital information server and a plurality of user systems are connected via a network~~,
A method for providing security, the method comprising:

receiving, at the ~~digital information~~ a server, a download request for digital information from one ~~user system~~ of a the plurality of user systems, each of the user systems being configured to generate a unique user key based on a system information of the user system the download request for digital information;

combining into a file an encrypted version of the digital information, a decryption key for decrypting the encrypted version of the digital information, and a rule corresponding to the digital information, wherein the rule corresponding to the digital information includes authority of use of the digital information and includes authority of transfer indicating whether the one user system can transfer the digital information to another user system;

transmitting the file from the ~~digital information~~ server to the one user system in response to the download request;

decrypting at the one user system the encrypted version of the digital information by the use of the decryption key; and

utilizing at the one user system the digital information in accordance with the rule corresponding to the digital information, and

transferring the digital information from the one user system to another user system in accordance with the rule corresponding to the digital information.

34. (Currently Amended) The ~~digital information security~~ method as claimed in according to claim 33, further comprising:

setting, using the ~~digital information~~ server, a plurality of groups, each group including a plurality of user systems; and

establishing, using the ~~digital information~~ server, a plurality of rules, each rule of the plurality of rules corresponding to each group; ,wherein the one user system is in one of the groups, wherein the rule corresponding to the digital information includes the rule corresponding to the group[[;]].

35. (Currently Amended) The ~~digital information security~~ method as ~~claimed in~~ according to claim 33, wherein the decryption key in the file and the rule corresponding to the group in the file are encrypted.

36. (Currently Amended) The ~~digital information security~~ method as ~~claimed in~~ according to claim 35, wherein the decryption key in the file and the rule corresponding to the group in the file ~~may can~~ be decrypted using a unique user key created using unique system information of the one user system.

37. (Currently Amended) ~~the digital information security~~ The method as ~~claimed in~~ according to claim 36, wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, RAM (Random Access Memory) information, unique HDD (Hard Disk Drive) information, and or serial number information of the one user terminal system.

38. (New) The server system according to claim 20, further comprising:

an encryption unit configured to encrypt data, a user information database configured to store the user information including the unique user key received from the user terminal for registration, a database configured to store the encrypted data, a rule establishing unit configured to establish a rule corresponding to the user information and the data, a coupling unit configured to encrypt, using the unique user key, rule information corresponding to the rule, and to encrypt, using the unique user key, a decryption key for decrypting the data, and to combine the encrypted rule information, wherein the encrypted decryption key and the encrypted data combined into information, and a digital file database configured to store the combined information; and

the server system further comprising a server control unit including a user management tool configured to perform a user authentication process by comparing the unique user key stored in the user information database with the unique user key subsequently transmitted from the user terminal for authentication,

wherein the server control unit transmits the combined information from the digital file database to the user application tool after completing the user authentication process, when the user terminal requests a download of the data.

39. (New) The method according to claim 24, further comprising:

encrypting data and the user information including the unique user key transmitted from the user terminal;

storing the encrypted user information and the encrypted data in the server system;

establishing a rule corresponding to the user information and the data;

encrypting the rule and a decryption key for decrypting the digital information using the unique user key;

combining the encrypted data, the encrypted rule and the encrypted decryption key into combined information;

storing the combined information;

performing a user authentication process by comparing the unique user key stored in the server with the unique user key subsequently transmitted from the user application tool of the user terminal for authentication;

transmitting the combined information from the server system to the user application tool via the network after completing the user authentication process, when the user terminal requests a download of the data; and

determining, with the user application tool, whether the data should be decrypted by determining whether the key used for encrypting the decryption key matches the unique user key created by the user application tool.

40. (New) The method for downloading data according to claim 30, further comprising:

performing a user authentication process at the server system by comparing a unique user key stored in the server system with the unique user key transmitted from the user terminal;

transmitting a digital file from the server to the user terminal when the user terminal is authenticated, the digital file including an encrypted version of the digital information data and

an encrypted decryption key, the decryption key for decrypting the encrypted version of the digital information data; and

decrypting, at the user terminal, the encrypted version of the digital information data if the key used for encrypting the decryption key matches with the unique user key created by the user application tool.